

LATHAM & WATKINS LLP
Lisa K. Nguyen (Bar No. 244280)
lisa.nguyen@lw.com
140 Scott Drive
Menlo Park, California 94025
Telephone: +1.650.328.4600
Facsimile: +1.650.463.2600

LATHAM & WATKINS LLP
Bob Steinberg (Bar No. 126407)
bob.steinberg@lw.com
Daniel Scott Schecter (Bar No. 171472)
daniel.schecter@lw.com
10250 Constellation Boulevard, Suite 1100
Los Angeles, California 90067
Telephone: +1.424.653.5500
Facsimile: +1.424.653.5501

Attorneys for Plaintiff
Monolithic Power Systems, Inc.

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

MONOLITHIC POWER SYSTEMS, INC., a
Delaware corporation;

Plaintiff,

v.

YAT TAM, an individual;

Defendant.

CASE NO.

COMPLAINT FOR:

**1) MISAPPROPRIATION OF TRADE
SECRETS (DEFEND TRADE SECRETS
ACT, 18 U.S.C. §§ 1836, *ET SEQ*);**

2) BREACH OF CONTRACT

DEMAND FOR JURY TRIAL

INTRODUCTION

1
2 1. Plaintiff Monolithic Power Systems, Inc. (“MPS”) is an industry leader in
3 providing power solutions for industrial applications, telecom infrastructures, cloud computing,
4 automotive, and consumer applications. To thrive in such a business, MPS develops proprietary
5 technology processes and confidential information to maintain its competitive advantage.
6 Consequently, in the course of their employment, MPS’s employees are entrusted with highly
7 confidential information and trade secrets.

8 2. One such employee was Defendant Yat Tam (“Defendant” or “Tam”). Defendant
9 worked for MPS as a product marketing manager from approximately June 2018 until July 2021,
10 when she resigned. MPS entrusted Defendant with trade secrets and other proprietary
11 information, and MPS relied on her promises to keep them confidential. Defendant betrayed that
12 trust. Just days before Defendant was to leave MPS, MPS discovered that Defendant
13 downloaded at least 60,000 files, including confidential and proprietary information. Most of
14 these downloaded documents and information had no relation to Defendants’ role at MPS,
15 causing particular concern.

16 3. When MPS confronted Defendant about her actions in connection with her exit
17 from the company, Defendant initially denied downloading any files, but eventually confessed.
18 Defendant then provided MPS with a hard drive, claiming that she had no other confidential
19 documents in her possession. Defendant also signed a document attesting that she had returned
20 all of MPS’s proprietary information. But Defendant’s signed attestations have proven false.

21 4. After Defendant left MPS, a forensic examination of her work laptops revealed
22 further misappropriation of MPS’s confidential trade secrets and retention of company
23 confidential and proprietary information, in breach of her agreement not to do so. Specifically,
24 the forensic examination revealed that, while still at MPS, Defendant had downloaded
25 documents and information to at least two other devices. Upon discovering this, MPS again
26 confronted Defendant and Defendant surrendered these drives to MPS. Another forensic
27 examination revealed that one of the drives—this time a USB drive—contained additional copies
28 of the same confidential and proprietary documents she had previously returned, as well as

additional confidential and proprietary MPS documents.

5. MPS has given Defendant multiple opportunities to disclose exactly what she had taken from MPS and to return all confidential trade secrets and other proprietary information. Instead of doing so, Defendant has continued to obfuscate the true extent of her misappropriation of MPS's confidential and proprietary information and trade secrets. It remains unknown how many additional copies of MPS's trade secrets and other confidential information Defendant still has, their location, or whether she has disclosed all devices or platforms where she stored company information.

6. Accordingly, MPS brings this action and asserts two causes of action against Defendant: (1) violation of the Defend Trade Secrets Act (“DTSA”), 18 U.S.C. §§ 1836, *et seq.*; and (2) breach of contract for violating the Parties’ Confidential Information and Invention Assignment Agreement (“Confidentiality Agreement”).

PARTIES

7. Plaintiff Monolithic Power Systems, Inc. (“MPS”) is a Delaware corporation with a place of business located at 79 Great Oaks Blvd., San Jose, California 95119. MPS provides power solutions for industrial applications, telecom infrastructures, cloud computing, automotive, and consumer applications, including to customers in interstate and foreign markets.

8. Defendant Yat Tam is an individual who lives in Mountain View, California and is a citizen of California. Defendant Tam is a former employee of MPS who, in violation of her contractual obligations to MPS, misappropriated MPS's trade secrets and confidential information. Defendant is currently employed by another technology company, Palo Alto Networks.

JURISDICTION

9. This Court has original jurisdiction over this action pursuant 28 U.S.C. § 1331 because this action involves claims under the DTSA, 18 U.S.C. §§ 1836, *et seq.*, and concerns trade secrets that relate to services or products that are used in or intended for use in interstate and foreign commerce.

10. This Court has supplemental jurisdiction over MPS's breach of contract claim

1 pursuant to 28 U.S.C. § 1367 because this claim forms part of the same case or controversy and
2 arises from the same series of events as those described in MPS's DTSA claim.

3 VENUE

4 11. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant
5 resides in the Northern District of California and a substantial portion of the events giving rise to
6 the claim occurred in the Northern District of California.

7 FACTUAL ALLEGATIONS

8 12. Plaintiff MPS provides ease of use power solutions in Cloud Computing,
9 Telecom, Industrial and Automotive market segments. Founded in 1997, MPS is a technical
10 leader in Integrated Power Semiconductor and Systems Power delivery architectures in the
11 world. MPS's founder, Michael Hsing, began with a belief that an entire power system could be
12 integrated into a single chip. Over twenty years later, MPS has succeeded not only in developing
13 a monolithic power module that truly integrates an entire power system into a single package, but
14 also continues to defy industry expectations with its proprietary groundbreaking technologies.
15 MPS accomplishes its mission through its employees—creative thinkers who break boundaries
16 and take technology to new levels. Using innovative, proprietary technology processes, MPS re-
17 imagines and re-defines the possibilities of high-performance power solutions in industrial
18 applications, telecom infrastructure, cloud computing, automotive, and consumer applications.
19 MPS is devoted to providing industry-leading, cutting-edge solutions to improve the quality of
20 life with green, easy-to-use products.

21 13. Due to the technical nature of its work, MPS develops proprietary technology and
22 large quantities of confidential data, including trade secrets. MPS uses this information,
23 including its trade secrets, to create and distribute its products and services to customers
24 throughout the United States and the world. Inevitably, during their employment, MPS's
25 employees encounter highly confidential information and trade secrets. For example, as part of
26 their employment, MPS's employees use their credentials to access MPS's non-public servers
27 which contain confidential and proprietary information about MPS and MPS's customers'
28 technology, products, and businesses.

14. MPS employed Defendant as a product marketing manager from June 2018 until July 2021. To ensure that MPS's confidential information and trade secrets remained protected from disclosure and to take reasonable steps to assure their secrecy, MPS required that Defendant enter into a confidentiality agreement as one of the terms of her employment.

15. Under the Confidentiality Agreement, which Defendant signed on or around June 25, 2018, Defendant agreed:

[1] at all times during [her] employment and thereafter, to hold in strictest confidence, and not to use, reproduce or copy, except for the benefit of the Corporation, or to disclose to any person, firm or corporation without written authorization of the Board of Directors of the Corporation, any Confidential Information of the Corporation, except under a non-disclosure agreement expressly authorized and executed by the Corporation[;] . . .

[2] not to keep, access, transmit, store, transfer, email, or otherwise maintain any Confidential Information of the Corporation on any system, device, storage media, computer, or server other than: (i) the computers owned and controlled exclusively by the Corporation and provided to [her] for [her] use in performing [her] duties during [her] employment at the Corporation; (ii) the secure servers owned and controlled exclusively by the Corporation and to which [she had] been granted access in performing [her] duties during [her] employment by the Corporation; and (ii[i]) other places (including drivers, servers, storage media, computers, systems, and devices) for which [she had] received the express, written advance approval from the Corporation's CEO[;] . . .

[and] [3] that, at the time of leaving the employ of the Corporation, [she would] deliver to the Corporation (and w[ould] not keep in [her] possession, recreate or deliver or cause to be delivered to anyone else) any and all Confidential Information, and all records, notes, reports, proposals, lists, correspondence, materials, other documents or property, or reproductions of any aforementioned items developed by [her] pursuant to [her] employment with the Corporation or otherwise belonging to the Corporation, [or] its successors or assigns

16. The Confidentiality Agreement defines "Confidential Information" to include:

any information the Corporation considers confidential and has not voluntarily disclosed or made available to the general public, including, without limitation, any sensitive business information, technical information, know-how, research, product development, product development opportunities, business plans, business or marketing strategies, product development strategies or plans, customer lists, markets, developments, inventions whether patentable or not, technical specifications, design layouts, schematics, data sheets, results of

1 simulations run, engineering notes, tests run and test results, source code,
2 designs, trade secrets, manufacturing specifications, internal customer
3 contact information, customer specifications (including purpose, design,
4 quantities requested or ordered, pricing, technical specifications, timing of
5 orders, budgets, and other information obtained from the customer resulting
6 from investment of time, effort, and money in developing such
7 information), financial information, or any other information relating to the
8 current and/or future business and operations of the Corporation.

9
10 17. Despite these contractual obligations, and Defendant's statutory obligations under
11 the DTSA, Defendant failed to honor her confidentiality obligations. Days before Defendant
12 resigned in July 2021, MPS discovered that Defendant had downloaded at least 60,000 files onto
13 a personal hard drive. These files are confidential to MPS. The majority of the files Defendant
14 downloaded had no connection to Defendant's role at MPS, and she had no legitimate reason to
15 access or use them.

16
17 18. During Defendant's exit interview, on July 9, 2021, MPS confronted Defendant
18 about the thousands of files she downloaded. Instead of confessing and explaining her actions,
19 Defendant initially lied and denied downloading the files. Eventually, however, Defendant
20 admitted that she downloaded the files and provided MPS with a hard drive, and claimed that she
21 had no other MPS documents or information in her possession. Additionally, Defendant signed a
22 Supplemental Employee Exit Interview Declaration ("Supplemental Declaration"), which
23 certified that she had "returned all documents, records, reports, data notebooks, proposals, lists,
24 correspondence, notes, compilations, sketches, blueprints, drawings, specifications, any
25 electronic storage devices, electronic files and other documents and all materials, tools,
26 equipment and any other property including any personal email accounts that contain
27 information, data, documents belonging to the Company and that [she] ha[d] no other Company
28 property in [her] possession[.]" Defendant also certified that she "ha[s] not and will not provide
any Confidential Information to any 3rd party, including [her] future employer(s)." Finally,
Defendant certified that she "reviewed a list of electronic files [MPS] provided to [her] . . . that
show [Defendant's] recent download activity on the MPS network," and she certified that she
"ha[s] or will return all of these electronic files to MPS and that [Defendant] ha[s] not and will

1 not provide any of these electronic files to any 3rd party, including [her] future employer(s).”

2 19. Defendant’s verbal and written confirmations were false. Following Defendant’s
3 departure, a forensic examination of her work laptops—which she returned at her July 9, 2021
4 exit interview—revealed that while at MPS, Defendant had downloaded other MPS documents
5 and information to at least two other external drives.

6 20. Upon making this discovery, MPS sent a letter to Defendant requesting that she
7 provide MPS with the two external drives identified in the forensic examination. Defendant
8 complied, providing MPS with the other two drives, including a USB drive. However, the USB
9 drive, which contained more than 20,000 files, only triggered new concerns.

10 21. The USB drive that Defendant provided contained not only additional copies of
11 the files she had previously “returned” in July, but also several new, confidential MPS files, all
12 of which had been transferred to the USB drive on September 9, 2021—the *same day* that MPS
13 requested the return of the drive and two months after Defendant left MPS. In other words,
14 despite Defendant’s verbal confirmation and written certification in the Supplemental
15 Declaration, she never returned all copies of the files she took in July. In fact, Defendant
16 remains in possession of the original files that she (wrongly) led MPS to believe that she had
17 returned, using yet another external storage device to transfer files to the USB drive on
18 September 9, 2021.

19 22. Still in possession of MPS’s confidential and proprietary information and trade
20 secrets, Defendant has now started working for another technology company, Palo Alto
21 Networks.

22 23. Defendant took files from MPS that include confidential and trade secret
23 information, including without limitation, information about MPS and MPS’s customers’
24 technology, products, and/or businesses (collectively, “MPS Trade Secrets”).

25 24. Given Defendant’s demonstrated deceit, MPS is understandably concerned that
26 Defendant’s misappropriation of the MPS Trade Secrets has only just begun. Accordingly, MPS
27 seeks relief for Defendant’s (1) violation of the DTSA, 18 U.S.C. §§ 1836, *et seq.*, and (2) breach
28 of the Confidentiality Agreement.

FIRST CAUSE OF ACTION

(Violation of the DTSA (18 U.S.C. §§ 1836, *et seq.*))

25. MPS re-alleges and incorporates by reference the allegations in paragraphs 1 through 24 as though fully set forth herein.

26. MPS's servers contain the MPS Trade Secrets. MPS uses the MPS Trade Secrets on its servers to create, provide, and/or distribute products and services used, sold, purchased, or transported, or intended for use, sale, purchase, or transport, in foreign and/or interstate commerce.

27. MPS is the owner of the MPS Trade Secrets, described above, which constitute "trade secrets" within the meaning of 18 U.S.C. § 1839(3).

28. As detailed more fully above in paragraphs 17 through 23, Defendant downloaded at least 60,000 files from MPS's servers that contain MPS Trade Secrets and other confidential information, and Defendant remains in possession of those files.

29. The above-detailed trade secret and confidential information that Defendant accessed, used, copied, forwarded, and/or downloaded, derives independent economic value, both actual and potential, from not being generally known to and not being readily ascertainable through proper means by MPS's competitors, who might obtain economic value from their disclosure or use.

30. At all times relevant herein, MPS has taken reasonable measures to protect the secrecy of the MPS Trade Secrets and its confidential information, including that which Defendant misappropriated.

31. Defendant gained access to the MPS Trade Secrets in the course of an employee-employer relationship between MPS and Defendant.

32. Defendant improperly acquired and retained the MPS Trade Secrets shortly before and upon resignation of her employment with Defendant.

33. Defendant's actions, as set forth herein, constitute "misappropriation" within the meaning of 18 U.S.C. § 1839(5).

34. Defendant accessed, used, copied, forwarded, and/or downloaded the MPS Trade

1 Secrets by improper means, without MPS's express or implied consent.

2 35. Defendant knew or had reason to know at the time she accessed, used, copied,
3 forwarded, and/or downloaded the MPS Trade Secrets that this information was acquired and
4 maintained by improper means and/or under circumstances giving rise to a duty to maintain
5 secrecy or limit use.

6 36. Defendant has failed to return to MPS the MPS Trade Secrets that she
7 misappropriated.

8 37. Defendant is retaining and/or using MPS's Trade Secrets to compete with and/or
9 otherwise harm MPS. As alleged herein, Defendant committed numerous acts in furtherance of
10 her misappropriation in this District, including misappropriating the MPS Trade Secrets in this
11 District with knowledge and intent to harm MPS.

12 38. Defendant's misappropriation has proximately caused damage to MPS, including
13 but not limited to, loss of profits, goodwill, competitive advantage, and business opportunities.

14 39. An order providing for the civil seizure of the MPS Trade Secrets, which are in
15 Defendant's possession, is justifiable under 18 U.S.C. § 1836(b)(2) because (1) Defendant's
16 repeated deception indicates that she would evade, avoid or otherwise not comply with an order
17 under Federal Rule of Civil Procedure 65 or another form of equitable relief, (2) MPS will suffer
18 an immediate and irreparable injury if such seizure is not ordered; (3) the harm to MPS of
19 denying the application outweighs the harm to the interests of Defendant and substantially
20 outweighs the harm to any third parties who may be harmed by such seizure; (4) MPS is likely to
21 succeed in showing that the MPS Trade Secrets in Defendant's possession qualify as trade
22 secrets and Defendant misappropriated the MPS Trade Secrets by improper means; (5)
23 Defendant has actual possession of the MPS Trade Secrets and the property to be seized; (6)
24 MPS has described with reasonable particularity the matter to be seized and the location where
25 the matter is to be seized; (7) Defendant would destroy, move, hide, or otherwise make the MPS
26 Trade Secrets inaccessible to the Court if MPS were to proceed on notice to Defendant; and (8)
27 MPS has not publicized the requested seizure.

28 40. Given Defendant's repeated misrepresentations to MPS and her evasion of its

1 attempts to regain possession of the MPS Trade Secrets that Defendant downloaded, an order
2 providing for the civil seizure of the MPS Trade Secrets, which are in Defendant's possession, is
3 justifiable under 18 U.S.C. § 1836(b)(2).

4 41. Defendant willfully and maliciously misappropriated the MPS Trade Secrets,
5 thereby justifying an award of punitive damages against Defendant pursuant to 18 U.S.C. §
6 1836(b)(3)(C) and attorneys' fees pursuant to 18 U.S.C. § 1836(b)(3)(D).

7 42. MPS is also entitled to temporary, preliminary, and/or permanent injunctive relief
8 to protect its confidential information and trade secrets by (1) enjoining Defendant from using or
9 disclosing the MPS Trade Secrets; (2) enjoining Defendant from altering or deleting the MPS
10 Trade Secrets; and (3) requiring Defendant to turn over any and all copies of the MPS Trade
11 Secrets.

12 **SECOND CAUSE OF ACTION**

13 **(Breach of Contract)**

14 43. MPS re-alleges and incorporates by reference the allegations in paragraphs 1
15 through 42 as though fully set forth herein.

16 44. Defendant and MPS entered a valid written contract—the Confidentiality
17 Agreement—on June 25, 2018. As described more fully above, in the Confidentiality
18 Agreement Defendant promised to protect MPS's confidential and proprietary information both
19 during and after Defendant's employment with MPS, including by returning all files to MPS
20 upon leaving MPS's employ.

21 45. Defendant downloaded information from MPS's servers, such as the MPS Trade
22 Secrets, that includes information MPS considers confidential and has not voluntarily disclosed
23 or made available to the general public. Defendant downloaded sensitive business information,
24 technical information, know-how, research, product development, product development
25 opportunities, business plans, business or marketing strategies, product development strategies or
26 plans, customer lists, markets, developments, inventions whether patentable or not, technical
27 specifications, design layouts, schematics, data sheets, results of simulations run, engineering
28 notes, tests run and test results, source code, designs, trade secrets, manufacturing specifications,

internal customer contact information, customer specifications (including purpose, design, quantities requested or ordered, pricing, technical specifications, timing of orders, budgets, and other information obtained from the customer resulting from investment of time, effort, and money in developing such information), financial information, and/or other information relating to the current and/or future business and operations of MPS.

46. Defendant breached the Confidentiality Agreement, including by taking, downloading, copying, reproducing, keeping, accessing, storing, transferring, and/or maintaining the information described above without MPS's permission during her employment.

47. Defendant also breached the Confidentiality Agreement by failing to deliver, keeping in her possession, recreating, delivering, and/or causing to be delivered the information described above while preparing to leave and after leaving the employ of MPS.

48. Defendant's breach has proximately caused damage to MPS, including but not limited to, loss of profits, goodwill, competitive advantage, and business opportunities.

PRAYER FOR RELIEF

WHEREFORE, MPS prays for judgment in its favor and against Defendant, inclusive, as follows:

1. Awarding damages as described in each of the above claims, in favor of MPS and against Defendant, in amounts to be determined at trial;
2. Granting temporary, preliminary, and/or permanent injunction against Defendant, requiring Defendant to return all misappropriated information and documents (and all material derivative from such information) to MPS and enjoining Defendant from further misappropriating or using the MPS Trade Secrets, and other such injunctive relief as may be proper;
3. An order providing for civil seizure of all misappropriated information and documents (and all material derivative from such information);
4. Awarding exemplary damages in favor of MPS and against Defendant in an amount to be determined at trial;
5. Awarding MPS pre- and post-judgment interest, attorneys' fees and costs, and

1 other expenses incurred in this action;

2 6. Granting MPS such other further relief as this Court deems just and proper.

3 **JURY DEMAND**

4 MPS demands a jury trial for all issues triable by jury.

5
6 Date: October 19, 2021

LATHAM & WATKINS LLP

7 By/s/ Lisa K. Nguyen

8 Bob Steinberg
9 Daniel Scott Schecter
Lisa K. Nguyen

10 Attorneys for Plaintiff
11 Monolithic Power Systems, Inc.
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28